Política de Segurança Digital

Orientações para o uso da Internet e dos dispositivos digitais em segurança e como recurso educativo.

Ficha Técnica:

Título: Política de Segurança Digital do Agrupamento de Escolas de Vila Viçosa

Edição Agrupamento de Escolas de Vila Viçosa

Vila Viçosa, janeiro de 2021

Aprovado pelo Conselho Pedagógico em janeiro de 2021

Índice

1. Objetivos e âmbito da Política de Segurança Digital

O Agrupamento de Escolas de Vila Viçosa, adiante designado apenas por Agrupamento, acredita que a Segurança Digital (eSafety) é um elemento essencial de salvaguarda das crianças, jovens e adultos no mundo digital, ao usar tecnologia, como computadores, tablets, telemóveis ou consolas de jogos.

O Agrupamento reconhece que a Internet e as tecnologias de informação e comunicação são uma parte importante da vida quotidiana, pelo que os alunos devem ser apoiados para serem capazes de aprender a desenvolver estratégias de gestão e resposta ao risco online.

O Agrupamento tem o dever, de acordo com as suas possibilidades técnicas e disponibilidade de recursos, de proporcionar à comunidade docente pontos de acesso à Internet de qualidade para elevar os padrões de educação, promover a realização de atividades, apoiar o trabalho profissional e melhorar as funções de gestão.

O Agrupamento identifica que há uma clara necessidade de garantir que todos os alunos e funcionários estão protegidos dos potenciais perigos online.

A política de segurança digital é, por isso mesmo, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar.

Este é documento é complementado por outro de nome "*Política de Privacidade e Proteção de Dados Pessoais".* Nesse documento são abordadas com maior pormenor as questões relativas à disponibilização dos dados pessoais dos alunos.

Os objetivos da **Política de Segurança Digital** (PSD) são:

- Identificar claramente os princípios fundamentais, seguros e responsáveis esperados de todos os membros da comunidade em relação à tecnologia como forma de garantir que o Agrupamento seja um ambiente seguro no que concerne à utilização de equipamentos eletrónicos e da Internet;
- Sensibilizar todos os membros do Agrupamento sobre os potenciais riscos, bem como dos benefícios da tecnologia;
- Permitir que todos os funcionários possam trabalhar com segurança e responsabilidade, com vista a um modelo comportamental positivo online, estando cientes da necessidade de gerir os seus próprios padrões e práticas ao usar a tecnologia;
- Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança online que são conhecidos por todos os membros da comunidade.

A PSD aplica-se a todos os funcionários, incluindo o órgão de gestão, professores, pessoal de apoio, prestadores de serviços, visitantes, voluntários e outras pessoas que trabalham para ou prestam serviços em nome do Agrupamento (coletivamente e adiante referidos como pessoal), bem como alunos e pais ou encarregados de educação.

Esta Política aplica-se a todos os dispositivos de acesso à Internet e utilização de dispositivos de comunicação e informação, incluindo dispositivos pessoais, ou outros que tenham sido fornecidos a alunos, funcionários ou outras pessoas.

Esta Política deve ser lida em conjunto com outras políticas escolares relevantes, incluindo (mas não limitada à salvaguarda e proteção da criança, *antibullying*, segurança de dados, e uso de imagem).

1.1. Redação e revisão da Política de Segurança Digital

- A definição, coordenação e implementação da PSD é da responsabilidade da Direção, a qual deve nomear um Coordenador de Segurança Digital.
- A Agrupamento reserva-se o direito de alterar, sem aviso prévio, a PSD que é discutida e aprovada em Conselho Pedagógico.
- A PSD foi redigida pelo Agrupamento, tendo por base a Política do Selo de Segurança Digital e a legislação em vigor.

1.2. A importância da utilização da *Internet*

- Devendo fazer parte integrante do currículo como uma ferramenta essencial no apoio à aprendizagem, a utilização da *Internet* no Agrupamento deve elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração escolar.
- O acesso à *Internet* é proporcionado aos alunos, sempre que possível, e estes deverão utilizá-la de forma responsável.
- Nas atividades de ensino e aprendizagem dever-se-á ensinar aos alunos o que é e o que não é uma utilização aceitável da *Internet*, e ser-lhes-ão indicados objetivos claros, quando utilizam a *Internet*, tendo em conta o currículo e a idade.
- A cópia, e a utilização subsequente de materiais obtidos na *Internet*, por alunos e professores, devem cumprir a legislação em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamentos disponíveis na *Web* e as regras de utilização dos recursos educativos abertos.
- O acesso à *Internet*, pelos alunos, faz-se única e exclusivamente pela VLAN[1] reservada para esse efeito na rede minedu, de modo a não por em causa a segurança dos dados dos professores, dos serviços administrativos e da Direção.
- Todas as atividades escolares que impliquem o uso da *Internet* devem permitir aos

[1] A infraestrutura de rede do AEVV é constituída por várias VLAN's de trabalho, diferenciando-se o acesso às mesmas por tipologia de utilizador (Alunos, Clientes Alunos Salas TIC, Clientes Professores, Clientes Administrativos e outras de segurança).

alunos aprender a pesquisar e a avaliar/validar informação, de acordo com a sua autoria, pertinência e rigor e devem ser adequadas, pelos professores, às diferentes faixas etárias.

- Todas as atividades escolares que impliquem o uso da *Internet* devem integrar a apresentação de referências bibliográficas normalizadas.

2. Gestão de sistemas de informação

2.1. Manutenção da segurança dos sistemas de informação

- A segurança dos sistemas informáticos do Agrupamento e dos utilizadores será revista regularmente.
- Os antivírus, nomeadamente os dos servidores, serão atualizados automaticamente e as licenças renovadas sempre que necessário.
- Os dados pessoais enviados através da *Internet* ou transferidos para fora da escola estão protegidos pelos sistemas de segurança dos programas utilizados, tendo em conta as recomendações da Comissão Nacional de Proteção de Dados, identificadas no nosso documento “Política de Privacidade e Proteção de Dados Pessoais”.
- Os dispositivos amovíveis serão utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática com antivírus.
- A instalação de software para fins educativos nos *Desktop* e portáteis deve ser autorizada pelo Coordenador da Segurança Digital e supervisionada, preferencialmente, por um dos assessores TIC ou por um professor de TIC.
- Os utilizadores não devem colocar / deixar ficheiros de uso pessoal nos PCs ou nos dispositivos móveis. Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos. Nos dispositivos móveis, os utilizadores também devem ter o cuidado de remover todas as contas pessoais associadas a aplicações.
- A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos, uma vez por ano letivo.
- É obrigatória a utilização de nomes de utilizador e palavras-passe para aceder à rede da escola.
- A página inicial de navegação de cada PC ao serviço dos utilizadores será definida pela direção, de acordo com as necessidades / interesses dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.

2.2. A gestão do correio eletrónico

- O Agrupamento disponibiliza contas de correio eletrónicas aos professores e funcionários e a comunicação institucional é feita por esta via.
- A comunicação com instituições para tratamento de assuntos oficiais do Agrupamento deve ser realizada a partir de endereços eletrónicos institucionais.
- Os grupos de contactos de correio eletrónico são geridos centralmente com o objetivo de facilitar o trabalho dos utilizadores.
- As mensagens de correio eletrónico enviadas para organizações externas devem obedecer a procedimentos de escrita e de protocolo similares aos do envio de ofícios por correio físico.
- A troca de mensagens com os alunos deve ser feita preferencialmente através de contas que não identifiquem diretamente os alunos.
- A troca de mensagens com encarregados de educação é feita para as suas contas pessoais.
- O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo dever ser cuidadosa, de modo a evitar ser objeto de *spam*.

2.3. Gestão dos conteúdos publicados

- As informações de contacto na página *Web* do Agrupamento devem ser a morada, os números de telefone e o *email* do Agrupamento. Não deve ser publicada qualquer informação pessoal de alunos ou professores.
- A publicitação *online* de horários das turmas e a listagem dos alunos das turmas só será efetuada se os sistemas garantirem um acesso restrito a alunos e a pais e encarregados de educação, com palavras-passe robustas. Não serão publicadas pautas online e as pautas afixadas em papel nos locais de estilo seguirão as recomendações da Comissão Nacional sobre Proteção de Dados relativas a faltas e outros dados de natureza pessoal.
- O Diretor é o responsável editorial geral pelos conteúdos digitais publicados pelo Agrupamento na *Internet* e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros do Agrupamento devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

2.4. Publicação de fotografias, de gravações de voz e de trabalhos de alunos

- Antes da publicação de imagens ou de gravações vídeo que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável.
- A publicação em linha, em rede aberta ou circuito fechado, de imagens dos alunos ou de gravações contendo a sua voz só são admissíveis se não houver uma relação direta entre a imagem e o som e o nome dos alunos, reduzindo, assim, significativamente, a possibilidade de identificação dos alunos.
- A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação.
- Os professores não devem recolher imagens ou voz dos alunos com os seus dispositivos pessoais e não podem publicar diretamente imagens ou outros registos dos alunos nas suas redes sociais pessoais.
- O consentimento por escrito será mantido pela escola, sempre que as imagens de alunos forem utilizadas para fins de publicidade, até as imagens em causa deixarem de ser usadas.
- Os trabalhos de alunos só serão publicados online com a autorização dos mesmos e dos pais / encarregados de educação das crianças e devem ter em conta as referências bibliográficas e os direitos de autor.

2.5. Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais

- Através de atividades dinamizadas pelos professores em sala de aula, nomeadamente nas aulas de TIC, e pelo Serviço das Bibliotecas Escolares, os alunos serão ensinados a usar a *Internet* e as redes sociais, de modo a protegerem a sua privacidade, a evitarem a divulgação de dados pessoais, a negarem o acesso a desconhecidos e a bloquearem comunicações não desejadas
- Os professores que pretendam utilizar ferramentas das redes sociais com os alunos em atividades curriculares devem avaliar o risco dos sítios na *Internet*, antes de os utilizarem e verificar os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos. Os blogues ou *wikis* oficiais geridos pelos professores devem estar protegidos por palavra-passe.
- Através da página *Web* do Agrupamento, serão feitas algumas campanhas de sensibilização de pais / encarregados de educação sobre a utilização segura de redes sociais e outros sítios de publicação de dados pessoais (dentro ou fora da escola), especialmente para os alunos mais novos. Estas ações de sensibilização para o uso seguro da *Internet* podem vir a ser organizadas em colaboração com as Associações de Pais e Encarregados de Educação do Agrupamento.

2.6. Gestão dos sistemas de filtragem

- O acesso à *Internet* fornecido pelo Agrupamento inclui sistemas de filtragem de conteúdos impróprios, implementados centralmente pela Direção-Geral de Estatísticas da Educação e Ciência que fornece o acesso à *Internet* e garante a manutenção regular destes sistemas de filtragem.
- Os professores que encontrarem sites bloqueados com interesse pedagógico ou sites impróprios que estão desbloqueados devem fazer chegar essa informação à Direção de modo a poder fazer-se o pedido de atualização à Direção-Geral de Estatísticas da Educação e Ciência.

3. Decisões quanto às políticas

3.1. Autorização do acesso à *Internet*

- Pessoal docente, não docente e alunos estão autorizados a aceder à *Internet,* desde do que o façam de forma responsável e no âmbito das suas funções.
- No ato da matrícula, os pais / encarregados de educação terão conhecimento da *Política de Segurança Digital* e da Política de Privacidade e Proteção de Dados Pessoais, disponíveis no sítio *Web* do Agrupamento e serão incentivados a analisá-los com os seus educados.

3.2. Resolução de incidentes relativos à Segurança Digital

- Todos os elementos do Agrupamento deverão informar o Coordenador da segurança digital se tiverem conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *cyberbullying*, conteúdos ilícitos, utilização inadequada de equipamento, etc).
- O Coordenador da segurança digital tomará as providências necessárias para resolver os incidentes de segurança digital, nomeadamente nos casos de cyber*bullying*.
- A aplicação de medidas para superação de problemas relativos à segurança digital, incluindo os que possam implicar a aplicação de medidas disciplinares, deve ser articulada com os responsáveis pelos serviços onde ocorreram os problemas.
- Alterações no acesso e nos serviços, decorrentes da aplicação de medidas no âmbito da segurança digital, devem ser comunicadas a alunos, docentes e pessoal não docente, ainda que com a devida proteção de confidencialidade das pessoas envolvidas.
- Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o Agrupamento contactará a Equipa de Proteção de Menores, através da Direção, e encaminhará a situação para as autoridades competentes.

3.3. Gestão dos casos de cyberbullying

- O *cyberbullying* não será tolerado e todos os incidentes detetados serão comunicados à Direção, ao Coordenador da Segurança Digital e às autoridades competentes, quando necessário.
- Aos alunos serão disponibilizadas atividades e sessões, dinamizadas por diferentes entidades do Agrupamento, de sensibilização para as questões do *cyberbullying*.

- Todos os incidentes de *cyberbullying* comunicados serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares, tal como estabelecido no Regulamento Interno.
- As sanções para os envolvidos em *cyberbullying* podem incluir:
    - A eliminação de todo o material considerado inapropriado pelo(a) autor(a) dos atos ou, caso se recuse ou não seja capaz de o fazer, eliminação realizada pelo fornecedor do serviço para que apague os conteúdos em questão;
    - O(A) autor(a) poderá ver o seu direito de acesso à *Internet* na escola suspenso durante um período de tempo a determinar pela Direção;
    - Os pais / encarregados de educação serão informados da sanção aplicada;
    - As autoridades competentes serão contactadas, caso se suspeite de ação ilícita.

3.4. Gestão de telemóveis e equipamentos pessoais

- Em sessões de sensibilização e atividades dirigidas a alunos, dinamizadas, quando possível, em articulação com as atividades curriculares, os alunos serão instruídos quanto à utilização segura e adequada de telemóveis e outros equipamentos pessoais e serão sensibilizados para os limites e consequências dos seus atos.
- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais (devendo, por isso, estar desligados), a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.
- A função de Bluetooth dos telemóveis deve estar sempre desligada e não pode ser utilizada para enviar imagens ou ficheiros para outros telemóveis ou para interferir com o funcionamento de outros dispositivos.
- Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para a escola. A escola não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos, nem por quaisquer efeitos prejudiciais para a saúde causados por estes dispositivos, sejam eles reais ou potenciais.
- Não é autorizado o uso de telemóveis e equipamentos pessoais em determinadas áreas dentro da escola, como vestiários ou casas de banho.
- Os professores podem confiscar um telemóvel ou equipamento, conforme o estabelecido no Código de Conduta do AE. O Coordenador de Segurança Digital pode fazer uma pesquisa ao telemóvel ou equipamento, com o consentimento do aluno ou dos pais / encarregados de educação. Caso se suspeite que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita, o telemóvel

será entregue às autoridades competentes para averiguações.

- No caso de apreensão, os telemóveis e outros equipamentos pessoais serão entregues aos pais / encarregados de educação.
- Não é permitido levar telemóveis e outros equipamentos para os exames. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos às normas estabelecidas pelo Júri Nacional de Exames.
- Se um(a) aluno(a) necessitar de contactar os pais ou encarregado de educação, deve usar, preferencialmente, o telefone da escola ou contactar os pais ou encarregado de educação através do seu telemóvel, em período não letivo e fora de espaços como salas de aula, biblioteca, zonas comuns dos blocos e outros espaços onde possa perturbar o funcionamento dos serviços.
- Os pais e encarregados de educação não devem contactar os filhos para os telemóveis durante o horário letivo. Em caso de necessidade de contacto urgente devem usar o número de telefone da Escola.
- Os professores e educadores não devem preferencialmente utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças, jovens ou seus familiares dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações de emergência e quando outros meios de contacto não estejam operacionais.
- Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone da escola.
- Os telemóveis e outros equipamentos estarão desligados ou em modo de "silêncio", a comunicação *Bluetooth* estará “oculta” ou desligada e os telemóveis e outros equipamentos não serão utilizados em períodos letivos, exceto em situações de emergência, ou em atividades pedagógicas, desde que haja consentimento para tal de todas as partes envolvidas na atividade.

4. Conhecimento das políticas

- A Política de Segurança Digital está disponível, para conhecimento e consulta, no sítio *Web* do Agrupamento.
- O Agrupamento incentiva os docentes da escola a frequentar a formação atualizada e adequada sobre a utilização segura e responsável da *Internet*, disponibilizada pelo centro de formação e a promover atividades de esclarecimento junto do pessoal não docente, alunos e pais / encarregados de educação.
- No sítio *Web* do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da *Internet* e de equipamentos informáticos.
- O Agrupamento chamará a atenção dos pais para a sua Política de Segurança Digital, através dos canais que entender adequados, nomeadamente no ato de matrícula.